+

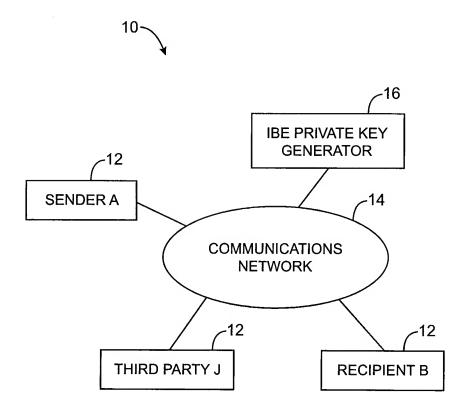


FIG. 1

+

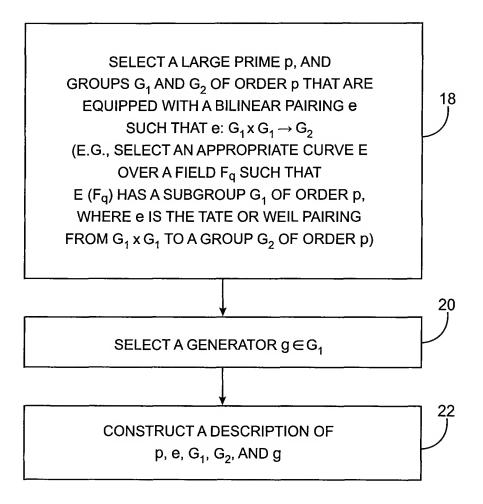


FIG. 2

+

3/8

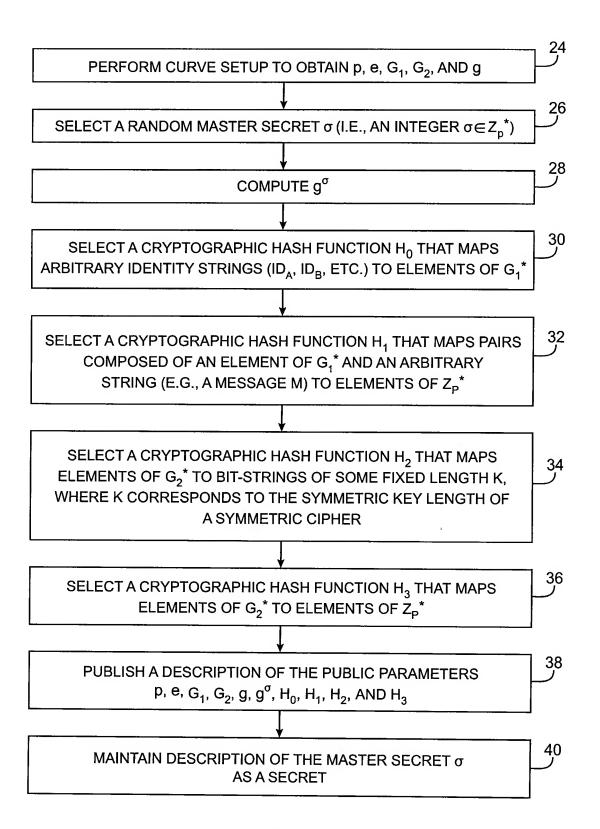


FIG. 3

+

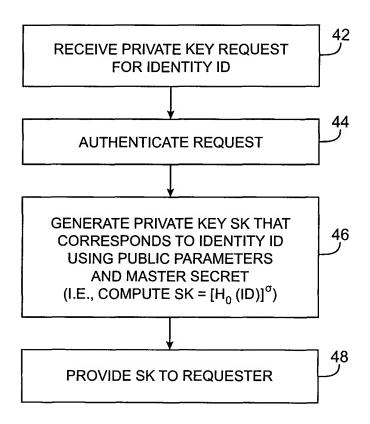


FIG. 4

5/8 50 PERFORM SIGNCRYPTION SETUP SENDER A OBTAINS IBE PRIVATE KEY SKA SENDER A SIGNS AND ENCRYPTS A MESSAGE M 54 TO CREATE A SIGNED AND ENCRYPTED VERSION OF MESSAGE M CALLED C (A USES IBE PUBLIC KEY OF RECIPIENT B AND A's IBE PRIVATE KEY SK_A) 56 SENDER A SENDS C TO RECIPIENT B ANONYMOUSLY 58 RECIPIENT B RECEIVES SIGNED AND ENCRYPTED MESSAGE C 60 RECIPIENT B OBTAINS IBE PRIVATE KEY SKR AND IBE PUBLIC PARAMETERS 62 RECIPIENT B DECRYPTS C TO PRODUCE IDENTITY OF SENDER A (ID_A), UNENCRYPTED MESSAGE M, AND IBE SIGNATURE OF M BY SENDER A (SIG_A (M)) -64 66 B PROVIDES ID_A , M, AND SIG_A (M) TO A THIRD PARTY J B VERIFIES SIG_A (M) TO PROVE THAT A SIGNED M AND TO VERIFY FOR B 68 (AND ONLY B) THAT J VERIFIES SIG_A (M) TO PROVE A CREATED C THAT A SIGNED M

FIG. 5

+

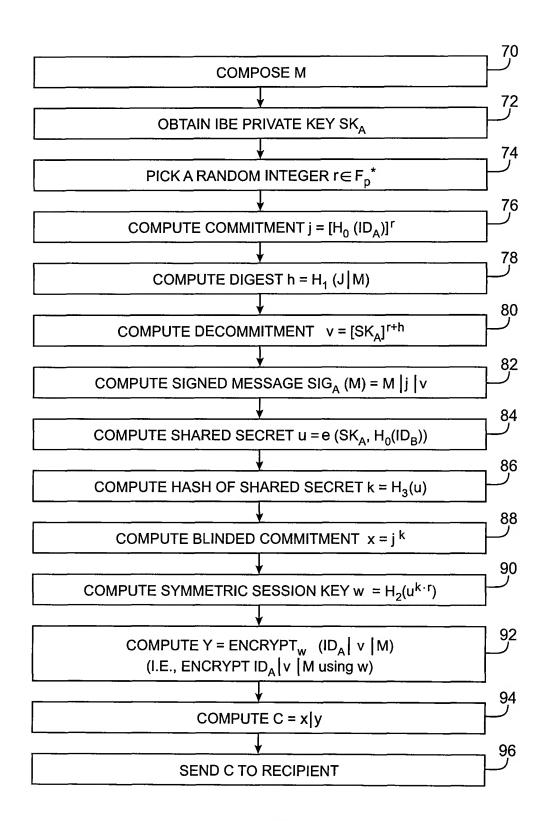


FIG. 6

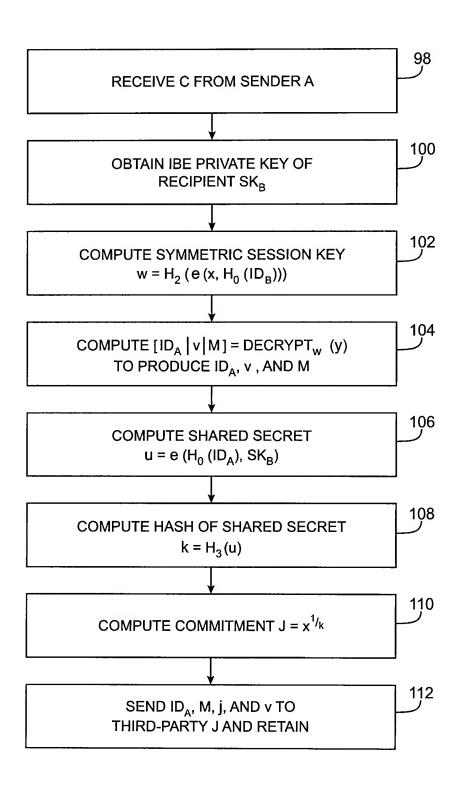


FIG. 7

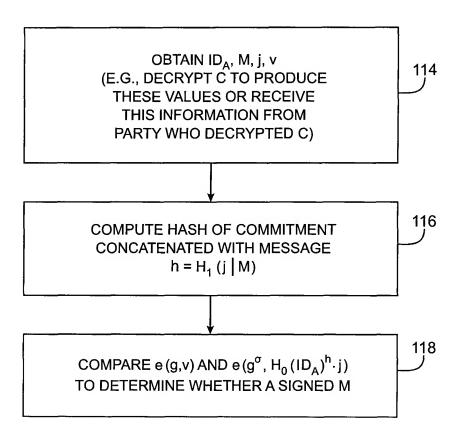


FIG. 8